

10/509,296

PATENT COOPERATION TREATY

PCT/FR2003/000937



Translation

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

 Rec'd PCT/PTO 24 SEP 2004
 (PCT Article 36 and Rule 70)

| | | |
|--|--|---|
| Applicant's or agent's file reference 344706D19955 | FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416) | |
| International application No. PCT/FR2003/000937 | International filing date (day/month/year) 25 mars 2003 (25.03.2003) | Priority date (day/month/year) 25 mars 2002 (25.03.2002) |
| International Patent Classification (IPC) or national classification and IPC G07F 19/00, G06F 17/60 | | |
| Applicant FRANCE TELECOM | | |

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.



This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 8 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

| | |
|--|---|
| Date of submission of the demand 26 septembre 2003 (26.09.2003) | Date of completion of this report 27 April 2004 (27.04.2004) |
| Name and mailing address of the IPEA/EP | Authorized officer |
| Facsimile No. | Telephone No. |

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR2003/000937

I. Basis of the report

1. This report has been drawn on the basis of (Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.):

- ☐ the international application as originally filed.
- ☒ the description, pages 1-19, as originally filed,
 pages _____, filed with the demand,
 pages _____, filed with the letter of _____,
 pages _____, filed with the letter of _____.
- ☒ the claims, Nos. _____, as originally filed,
 Nos. _____, as amended under Article 19,
 Nos. _____, filed with the demand,
 Nos. 1-32, filed with the letter of 12 February 2004 (12.02.2004),
 Nos. 20-27, filed with the letter of 12 February 2004 (12.02.2004).
- ☒ the drawings, sheets/fig 1/7-7/7, as originally filed,
 sheets/fig _____, filed with the demand,
 sheets/fig _____, filed with the letter of _____,
 sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 03/00937

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

| | | | |
|-------------------------------|--------|------|-----|
| Novelty (N) | Claims | 1-32 | YES |
| | Claims | | NO |
| Inventive step (IS) | Claims | 1-32 | YES |
| | Claims | | NO |
| Industrial applicability (IA) | Claims | 1-32 | YES |
| | Claims | | NO |

2. Citations and explanations

1. Reference is made to the following documents:

- D1: WO 00 75749 A (INTELLISHIELD.COM, INC.) 14 December 2000 (2000-12-14)
- D2: US-A-5 991 738 (OGRAM) 23 November 1999 (1999-11-23)
- D3: WO 01 80190 A (CYBERUN CANADA CORP.) 25 October 2001 (2001-10-25)
- D4: WO 02 05231 A (PAYPAL, INC.) 17 January 2002 (2002-01-17)
- D5: WO 01 08066 A (IPRIVACY LLC) 1 February 2001 (2001-02-01)
- D6: EP-A-1 026 644 (APPAGE CORPORATION) 9 August 2000 (2000-08-09)

2. The aim of the invention is to prevent the circulation, on the network and towards the merchant, of banking information relating to the holder's credit card, while minimising the involvement of the third party in the management of the transaction. D1, which is considered to be the most relevant prior art, describes a method for securing credit card transactions on a telecommunication network between a holder and a

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 03/00937

merchant according to the preamble of claim 1.

Consequently, the subject matter of claim 1 differs from this known method in that the holder contacts the third party before making contact with the merchant. The holder only makes contact with the merchant via the third party. The notion of the holder contacting the third party before contacting the merchant is not disclosed in D1.

This procedure is neither known from nor suggested by the prior art known from documents D1 to D6.

Claim 22 describes a system for securing credit card transactions implementing the method according to claim 1.

Claims 1 and 22 therefore meet the requirements of PCT Article 33(2) and (3).

3. Claims 2 to 21 are dependent on claim 1 and claims 23 to 32 are dependent on claim 22 and thus also comply, as such, with the requirements of novelty and inventive step of the PCT.

CLAIMS

1. A method for secure credit card transactions between a holder (5) and a merchant (7), particularly via a telecommunication network (9), by entering in the order form supplied by the merchant (7), during the payment phase of the transaction, temporary information consistent with the bank information from the card of the holder (5), this temporary information then being collected by an authorization center for the transaction in order to make a relational connection with the real bank information from the card of the holder for the acknowledgement of the order by the holder (5) for the benefit of the merchant (7), characterized in that it comprises the steps in which:
- the holder (5) signifies to a third party (6) his intention to enter into contact with the merchant (7) before entering into contact with the merchant (7) over the telecommunication network (9);
 - the holder (5) enters into contact with the merchant (7) through the third party (6);
 - the third party (6) establishes a link between itself and the holder (5) and between itself and the merchant (7);
 - the third party (6) manages the formation of temporary information, the entry of this information in the order form and the relational connection of the temporary information with the real bank information from the credit card of the holder to check the various authorizations with the banks for the acknowledgement of the order.
2. The method as claimed in claim 1, characterized in that the link between the third party (6) and the holder (5) is secured in such a way as to allow

the third party to intercept and control all the information transmitted by the holder (5) to the merchant (7) via the third party, but in a manner transparent for the holder (5).

5

3. The method as claimed in either one of claims 1 or 2, characterized in that the link between the third party (6) and the merchant (7) is secured in such a way as to allow the third party to intercept and control all the information transmitted by the merchant (7) to the holder (5) via the third party, but in a manner transparent for the holder (5).

10

4. The method as claimed in claim 2, characterized in that the secure link between the holder (5) and the third party (6) is of the Secure Socket Layer type.

15

5. The method as claimed in claim 3, characterized in that the secure link between the merchant (7) and the third party (6) is of the Secure Socket Layer type.

20

6. The method as claimed in one of claims 1 to 5, characterized in that the holder (5) signifies his intention to enter into contact with the merchant (7) by making a connection with the site of the third party and/or by indicating the Internet address of the third party (6) in a telecommunication network browser.

25

30

7. The method as claimed in one of claims 1 to 6, characterized in that the third party (6) modifies the relative or absolute Internet addresses of the site of the merchant (7) to constrain the browser of the holder to systematically transmit to it all the information from the holder (5) to the merchant (7).

35

8. The method as claimed in one of claims 1 to 7, characterized in that the third party modifies the relative or absolute Internet addresses of the site of the merchant (7) to constrain the browser of the merchant to systematically transmit to it all the information from the merchant (7) to the holder (5).
9. The method as claimed in one of claims 1 to 8, characterized in that two order acknowledgement procedures are possible depending on whether the holder (5) has or has not previously registered with the third party (6), this registration comprising the transmission to said third party of the bank information concerning the holder and his credit card in a register of the third party.
10. The method as claimed in claim 9, characterized in that, if the holder (5) has previously registered with the third party (6), he may choose not to indicate the bank information concerning him in the reserved domain of the order form of the transaction, and consequently not to complete said domain other than by an identifier with the third party, the portion requiring bank information being completed by the third party with temporary and coherent information, only this temporary information being sent to the merchant (7).
11. The method as claimed in one of claims 1 to 10, characterized in that a procedure of verifying the intention of the holder to carry out the transaction is triggered.
12. The method as claimed in claim 11, characterized in that the verification comprises a step in which the holder (5) is called back on his mobile telephone, the holder signifying his agreement to

the third party by entering a password which may be returned thanks to a short message on mobile telephone and/or an electronic signature produced by the mobile telephone.

- 5
13. The method as claimed in claim 11, characterized in that the verification comprises a step in which the holder enters in a secure window a password on the means connected to the telecommunication network.
- 10
14. The method as claimed in claim 11, characterized in that the verification comprises a step in which an email is sent to the holder, the holder then having to return the email with an identifier used to confirm the transaction.
- 15
15. The method as claimed in claim 11, characterized in that the verification comprises a step in which the cryptographic signature of means that the holder has in his possession is verified, particularly a smart card inserted into a reader connected to the telecommunication network.
- 20
- 25 16. The method as claimed in claim 9, characterized in that, if the holder is not registered with the third party, he enters the bank information from his credit card in the order form supplied by the merchant via the third party, the third party then managing the completion of the order form which will be sent to the merchant with temporary information.
- 30
- 35 17. The method as claimed in one of claims 1 to 16, characterized in that it comprises the steps in which:
- a bank authorization center (602) connected to the third party (6) collects the bank authorization request, that comes from the

ART 34 AMDT

- merchant (7) or from the bank of the merchant and that contains the temporary information;
- said bank authorization center carries out a conversion making a relational connection of the temporary information with the real bank information;
 - it sends the real bank information of the holder to the bank authorization center of the holder;
 - it retrieves the response from the bank authorization center of the holder containing the real bank information;
 - it makes a conversion in order to remake a relational connection of the real bank information with the temporary information;
 - it returns to the merchant or to the authorization center of the bank of the merchant the response of the bank authorization center of the holder containing the temporary information.
18. The method as claimed in one of claims 1 to 17, characterized in that periodically the center for collecting the transactions of the merchant (7) sends all the transactions made between said merchant and holders via the third party to a collection center linked to the third party, the third party again converting the temporary information into the real bank information of the various holders, the collection center linked to the third party then redistributing the transactions to the various collection centers of the banks of the holders.
19. The method as claimed in one of claims 1 to 18, characterized in that the authorization center of the holder also comprises a Bank Client Profile module which receives, via a secure link, the bank authorization requests originating from the authorization center connected to the third party, this module being configured by the authorization

request center connected to the third party so that it gives to the authorization center of the holder information for the release, transaction by transaction, of an interdiction to acknowledge the transactions made by the holder via the telecommunication network.

20. The method as claimed in one of claims 1 to 19, characterized in that the bank information is the number and expiry date of the credit card.

21. The method as claimed in one of claims 1 to 20, characterized in that the bank of the holder intervenes during the transactions between the holder and the merchant, by offering the holder services relating to the transaction.

22. A system for secure credit card transactions between a holder (5) and a merchant (7), particularly via a telecommunication network (9), comprising means forming a third party (6) connected via the network (9) between the holder (5) and the merchant (7), the third party comprising means for simultaneously establishing a link between itself (6) and the holder (5) and between itself (6) and the merchant (7), the third party also comprising means for forming temporary information consistent with the bank information from the card of the holder (5), the system comprising means forming a center for authorizing the transaction and suitable for collecting this temporary information in order to place it in a relational connection with the real bank information from the card of the holder (5) for the acknowledgement of the order by the holder to the benefit of the merchant, characterized in that it comprises means suitable for allowing the holder (5) to signify to the third party (6) his intention to enter into contact with the merchant

ART 34 AMDT

- 26 -

- 5 (7) before entering into contact with the merchant
(7) over the telecommunication network (9), and
the third party comprises means suitable for
entering in the order form the temporary
information consistent with the bank information
from the card of the holder (5).
- 10 23. The system as claimed in claim 22, characterized
in that it also comprises means for intercepting
and controlling all the information transmitted by
the holder to the merchant.
- 15 24. The system as claimed in either one of claims 22
or 23, characterized in that it comprises means
for securing the link between the third party and
the holder suitable for allowing the third party
to intercept and control all the information
transmitted by the holder (5) to the merchant (7)
via the third party, but in a manner transparent
20 for the holder (5).
- 25 25. The system as claimed in one of claims 22 to 24,
characterized in that it comprises means for
securing the link between the third party and the
merchant suitable for allowing the third party to
intercept and control all the information
transmitted by the merchant (7) to the holder (5)
via the third party, but in a manner transparent
for the holder (5).
- 30 26. The system as claimed in one of claims 22 to 25,
characterized in that the secure link between the
holder (5) and the third party (6) is of the
Secure Socket Layer type.
- 35 27. The system as claimed in one of claims 22 to 26,
characterized in that the secure link between the
merchant (7) and the third party (6) is of the
Secure Socket Layer type.

MODIFIED SHEET

ART 34 ADDI

28. The system as claimed in one of claims 22 to 27,
characterized in that the holder (5) comprises
means suitable for establishing a connection with
the merchant (7) via a connection on the site of
the third party and/or suitable for entering the
Internet address of the third party (6) in a
telecommunication network browser.
29. The system as claimed in one of claims 22 to 28,
characterized in that the third party comprises
means suitable for modifying the relative or
absolute Internet addresses of the site of the
merchant (7) and suitable for constraining the
browser of the holder to systematically transmit
to it all the information from the holder to the
merchant (7).
30. The system as claimed in one of claims 22 to 29,
characterized in that the third party comprises
means suitable for modifying the relative or
absolute Internet addresses of the site of the
merchant (7) and suitable for constraining the
browser of the merchant to systematically transmit
to it all the information from the merchant (7) to
the holder (5).
31. The system as claimed in one of claims 22 to 30,
characterized in that it comprises:
- means forming a bank authorization center (602)
connected to the third party and collecting the
bank authorization request that comes from the
merchant or from his bank and that contains the
temporary information;
 - means (601) suitable for carrying out a
conversion making a relational connection of the
temporary information with the real bank
information;
 - means suitable for sending the real bank

ART 34 ART

- 28 -

information of the holder to the bank authorization center of the holder;

- means suitable for retrieving the response from the bank authorization center of the holder containing the real bank information;
- means suitable for carrying out a conversion in order to remake a relational connection of the real bank information with the temporary information;
- means suitable for returning to the merchant or to the authorization center of his bank the response from the bank authorization center of the holder containing the temporary information.

32. The system as claimed in one of claims 22 to 31, characterized in that the means forming the authorization center of the holder also comprise a Bank Client Profile module suitable for receiving, via a secure link, the bank authorization requests originating from the authorization center connected to the third party, this module being suitable for being configured by the authorization request center connected to the third party so that it gives to the authorization center of the holder information for the release, transaction by transaction, of an interdiction to acknowledge the transactions made by the holder via the telecommunication network.